

Experimental Constructions of Binary Matrices with Good Peak-Sidelobe Distances

Jerod Michel *

September 16, 2016

Abstract

Skirlo et al., in “Binary matrices of optimal autocorrelations as alignment marks” [*Journal of Vacuum Science and Technology Series B* 33(2) (2015) 1-7], defined a new class of binary matrices by maximizing the peak-sidelobe distances in the aperiodic autocorrelations and, by exhaustive computer searches, found the optimal square matrices of dimension up to 7×7 , and optimal diagonally symmetric matrices of dimensions 8×8 and 9×9 . We make an initial investigation into and propose a strategy for (deterministically) constructing binary matrices with good peak-sidelobe distances. We construct several classes of these and compare their distances to those of the optimal matrices found by Skirlo et al. Our constructions produce matrices that are near optimal for small dimension. Furthermore, we formulate a tight upper bound on the peak-sidelobe distance of a certain class of circulant matrices. Interestingly, binary matrices corresponding to certain difference sets and almost difference sets have peak-sidelobe distances meeting this upper bound.

Key words and phrases: Difference sets, almost difference sets, binary matrices, aperiodic autocorrelation, cyclotomic cosets.

Mathematics subject classifications: 05B05, 05B10, 11T22, 51E30, 05B30, 94C30.

1 Introduction

Sequences and matrices with good autocorrelation properties have important applications in digital communications such as radar, sonar, code-division multiple access (CDMA), and cryptography [2], [12], as well as in coded aperture imaging [9]. A less developed problem in matrix design was recently considered by Skirlo et al. in [15]. Here, the application of binary matrices with good aperiodic autocorrelation properties to two-dimensional spatial alignment is noted, where an alignment mark is made by creating a surface pattern different from the background thereby allowing pattern information to transform into a two-level signal while a digital image is taken. Position marks for electron-beam

*J. Michel is with the Department of Mathematics, Zhejiang University, Hangzhou 310027, China (e-mail: contextolibre@gmail.com).

lithography based on such binary matrices, for example, were shown to be immune to noise and certain manufacturing errors in [3], but the elements of the application have yet to be optimized. So far, such matrices have been obtained only by exhaustive computer searches.

Let I and J be index sets with $|I| = M$ and $|J| = N$. Let $R = (R_{i,j})$ be an M by N binary matrix whose rows and columns are labelled by I and J respectively. The 2D aperiodic autocorrelation $A_R(\tau_1, \tau_2)$ at integer shifts τ_1 and τ_2 of the binary matrix R is given by

$$A_R(\tau_1, \tau_2) = \sum_{i \in I} \sum_{j \in J} R_{i,j} R_{i+\tau_1, j+\tau_2}. \quad (1)$$

Note that $(A_R(\tau_1, \tau_2))$ is an inversion-symmetric $(2M - 1) \times (2N - 1)$ matrix, i.e., $A_R(\tau_1, \tau_2) = A_R(-\tau_1, -\tau_2)$ for all τ_1, τ_2 . Also note that all the matrices are implicitly padded with 0s for all the matrix elements of indices exceeding their matrix dimensions. The crosscorrelation between the matrix R and the data image matrix R' is given by

$$C_{RR'}(\tau_1, \tau_2) = \sum_{i=1}^M \sum_{j=1}^N R_{i,j} R'_{i+\tau_1, j+\tau_2}.$$

If the data matrix R' is a noisy version of the reference matrix R , the peak value of the crosscorrelation can determine the most probable position of the mark.

The aperiodic autocorrelation of a binary matrix can be expressed as $\{d_1 | n_1, n_2, \dots, n_{s+1}\}$. Here $d_1 = l - s$ where l is the number of 1s in the binary matrix, called the *peak*, and s is the highest value of $A_R(\tau_1, \tau_2)$ for τ_1, τ_2 not both zero, called the *nearest sidelobe*. The other distances are given by $d_{i+1} = d_i + 1$ for $i \geq 1$, where n_i gives the number of times d_i occurs in the autocorrelation.

1.1 Previous Work

In [15], two criteria are given for a binary matrix to be optimal; one is that the probability of misalignment, which depends on the values of the sidelobes of the autocorrelation, should be minimized, and the other is that the misalignment deviation, which depends on the positions of the sidelobes relative to the peak value $A_R(0, 0)$, should be minimized. Therefore, binary matrices with an autocorrelation $\{d_1 | n_1, n_2, \dots, n_{s+1}\}$ in which

1. d_1 is maximized, and
2. the n_i s are minimized sequentially in the dictionary order,

are desirable. Matrices of any sizes can be compared using these criteria.

In [15], two upper bounds which depend on the number of 1s in the matrix were computed. Skirlo et al. found that the largest possible d_1 for all matrices with given l (number of 1s in the matrix) and fixed dimension, is $d_{1,max} = l - s_{min}(l)$ where $s_{min}(l)$ is the minimum highest sidelobe value as a function of l . The first upper bound, $d_{1,max}^{upper,I}(l)$ was computed by maximizing $l - A_R(\pm 1, 0)$. By

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Figure 1: 6×6 and 7×7 optimal binary matrices

computing $A_R(\pm 1, 0)$ a lower bound $s_{min}^{lower, I}(l)$ on $s_{min}(l)$ is obtained. Assuming $M \leq N$ the first upper bound on $d_{1, max}(l)$ was found to be

$$d_{1, max}^{upper, I}(l) = \begin{cases} l, & l \in [0, N_1] \\ N_1, & l \in [N_1, N_2] \\ M(N+1) - l, & l \in [N_2, MN] \end{cases} \quad (2)$$

where $N_1 = \frac{MN}{2}$, $N_2 = \frac{MN}{2} + M$ when MN is even and $N_1 = \frac{MN+1}{2}$, $N_2 = \frac{MN+1}{2} + M - 1$ if MN is odd. The other upper bound that was found in [15] has similar dependencies. The drawbacks of these upper bounds are that they are not tight, which can easily be seen by checking any of the peak-sidelobe distances of the optimal matrices they found against the bound, and that they are functions of l and not just M and N . The aperiodicity of the autocorrelation function makes the problem of formulating a tight upper bound that depends only on the dimension of the binary matrix difficult.

1.2 Overview of Proposed Strategy

Here we propose a strategy for an initial investigation into the problem of constructing binary matrices with good peak-sidelobe distances. Concerning the $M \times M$ optimal matrices found in [15], three important observations can be made: the first is that most of them are diagonally-symmetric, the second is that the nearest sidelobe always occurs within $\{A_R(\pm 1, 0), A_R(0, \pm 1)\}$, and the third is that they all consist of an *interior* $((M-2) \times (M-2))$ matrix obtained by deleting the first and last row and the first and last column) in which each row and column has roughly the same number of 1s, and an *exterior* (first and last row, and first and last column) in which every entry is a 1 except for possibly one 0 on each side. These observations are illustrated in Figure 1 by the optimal binary matrices of dimensions 6×6 resp. 7×7 that were found in [15].

This first and third observations lead us to consider the following general method for constructing a binary $M \times M$ matrix with a good peak-sidelobe distance:

Step 1: Construct an $(M-2) \times (M-2)$ circulant matrix whose peak-sidelobe distance is large among the class of all $(M-2) \times (M-2)$ circulant matrices.

Step 2: Obtain an $M \times M$ matrix by giving a border of 1s to the matrix obtained in Step 1.

Step 3: Try to increase the peak-sidelobe distance of the matrix obtained in Step 2 by changing some of the 1s on the border to 0s.

Since computing the peak-sidelobe distance at an arbitrary shift is troublesome due to the aperiodicity of the autocorrelation, the second observation mentioned above suggests considering, as the interior matrix, circulant matrices whose nearest sidelobe occurs within $\{A_R(\pm 1, 0), A_R(0, \pm 1)\}$. This ensures that the peak-sidelobe distance will be $A_R(0, 0) - A_R(\tau'_1, \tau'_2)$ where $A_R(\tau'_1, \tau'_2) \in \{A_R(\pm 1, 0), A_R(0, \pm 1)\}$. It turns out that if we assume the interior matrix is a circulant matrix such that in each row (or column), the number of pairs of consecutive 1s is large enough, the nearest sidelobe will occur in $\{A_R(\pm 1, 0), A_R(0, \pm 1)\}$. We formulate a tight upper bound for the peak-sidelobe distance of such a circulant matrix and, interestingly, circulant matrices corresponding to certain difference sets and almost difference sets have peak-sidelobe distances meeting this upper bound. It turns out that we can find $(M - 2) \times (M - 2)$ circulant matrices whose peak-sidelobe distances are optimal among the class of all such $(M - 2) \times (M - 2)$ circulant matrices. Using such matrices as the interior matrix, after adjoining an exterior of 1s, and then carefully choosing which of these 1s to change to 0s, we obtain $M \times M$ binary matrices with peak-sidelobe distances that are good in the sense that they are very close to being optimal for small dimensions. We construct several families of such matrices and, for small dimensions, compare their peak-sidelobe distances to those of the optimal matrices found in [15].

In Section 2 we discuss some necessary preliminary concepts. In Section 3 we formulate a tight upper bound for the peak-sidelobe distance of a certain class of binary circulant matrices. In Section 4 we construct several binary circulant matrices with peak-sidelobe distances meeting the upper bound. In Section 5 we construct several families of binary matrices with good peak-sidelobe distances and, for small dimension, compare these to the peak-sidelobe distances of the optimal matrices found in [15]. Section 6 concludes the paper.

2 Preliminaries

2.1 Periodic Distance, Difference Sets and Circulant Matrices

Let G be an additive group of order v , and k a positive integer such that $2 \leq k < v$. A k -element subset $D \subseteq G$ has *difference levels* $\mu_1 < \dots < \mu_s =: \Lambda$ if there exist integers t_1, \dots, t_s such that the multiset

$$M = \{g - h \mid g, h \in D\}$$

contains exactly t_i members of $G - \{0\}$ each with multiplicity μ_i for all i , $1 \leq i \leq s$. The *periodic distance* of D , denoted $d(D)$, is defined by $d(D) = k - \Lambda$. We say that D is *cyclic* if G is cyclic. If D is cyclic and the number of pairs of consecutive residues in D is Λ , then we say D is *special*. In the case where $s = 1$, D is called a (v, k, Λ) *difference set* [10], and in the case where $s = 2$ and $\Lambda = \mu_2 = \mu_1 + 1$, D is called a (v, k, μ_1, t_1) *almost difference set* [13].

Theorem 2.1. [16] *The set D is a (v, k, λ) difference set in Abelian group G if and only if its complement D^c is a $(v, v - k, v - 2k + \lambda)$ difference set in G .*

Theorem 2.2. [1] *The set D is a (v, k, λ, t) almost difference set in Abelian group G if and only if its complement D^c is $(v, v - k, v - 2k + \lambda, t)$ almost difference set in G .*

We call the set $\{D + g \mid g \in G\}$ of translates of D , denoted by $Dev(D)$, the *development* of D . Let $R = (R_{g,h})$ be the $v \times v$ matrix defined by

$$R_{g,h} = \begin{cases} 1, & \text{if } g \in D + h, \\ 0, & \text{otherwise,} \end{cases}$$

for $g, h \in G$. Then we say R is the *incidence matrix* of $Dev(D)$. If G is cyclic then we say R is a *binary circulant matrix* with defining set D , and we say that a R is *special* if D is special.

2.2 Group Ring Notation

It is sometimes convenient to represent binary matrices by members of group rings. Let G be an additive Abelian group and \mathbb{Z} the ring of integers. Define the group ring $\mathbb{Z}[G]$ to be the ring of all formal sums

$$\mathbb{Z}[G] = \left\{ \sum_{g \in G} a_g X^g \mid a_g \in \mathbb{Z} \right\}$$

where X is an indeterminate. The ring $\mathbb{Z}[G]$ has the operation of addition given by

$$\sum_{g \in G} a_g X^g + \sum_{g \in G} b_g X^g = \sum_{g \in G} (a_g + b_g) X^g,$$

and the operation of multiplication defined by

$$\left(\sum_{g \in G} a_g X^g \right) \left(\sum_{g \in G} b_g X^g \right) = \sum_{h \in G} \left(\sum_{g \in G} a_g b_{h-g} \right) X^h.$$

We denote the unit of $\mathbb{Z}[G]$ by $X^{\mathbf{0}} = \mathbf{1}$ where $\mathbf{0}$ is an additive identity.

2.3 Cyclotomic Classes and Cyclotomic Numbers

Let q be a prime power, and γ a primitive element of \mathbb{F}_q . The *cyclotomic classes* of order e are given by $C_i^e = \gamma^i \langle \gamma^e \rangle$ for $i = 0, 1, \dots, e - 1$. Define $(i, j)_e = |C_i^e \cap (C_j^e + 1)|$. It is easy to see there are at most e^2 different cyclotomic numbers of order e . When it is clear from the context, we simply denote $(i, j)_e$ by (i, j) . The cyclotomic numbers (h, k) of order e have the following properties [4]:

$$(h, k) = (e - h, k - h), \quad (3)$$

$$(h, k) = \begin{cases} (k, h), & \text{if } f \text{ even,} \\ (k + \frac{e}{2}, h + \frac{e}{2}), & \text{if } f \text{ odd.} \end{cases} \quad (4)$$

We will also need the following lemmas.

Lemma 2.3. [13]

$$-D_i^e := \{-x \mid x \in D_i^e\} = \begin{cases} D_i^e, & \text{if } f \text{ is even} \\ D_{i+\frac{e}{2}}^e, & \text{if } f \text{ is odd.} \end{cases}$$

Lemma 2.4. [13] *Let $q = em + 1$ be a prime power for some positive integers e and f . In the group ring $\mathbb{Z}[\mathbb{F}_q]$ we have*

$$C_i^e(X)C_j^e(X^{-1}) = a_{ij}\mathbf{1} + \sum_{k=0}^{e-1} (j - i, k - i)_e C_k^e(X)$$

where

$$a_{ij} = \begin{cases} f, & \text{if } m \text{ is even and } j = i, \\ f, & \text{if } m \text{ is odd and } j = i + \frac{e}{2}, \\ 0, & \text{otherwise.} \end{cases}$$

3 A General Upper Bound on the Peak-Sidelobe Distance of a Special Matrix

We first formulate the following general upper bound on the periodic distance of a subset of a cyclic group.

Lemma 3.1. *Let D be a k -subset of \mathbb{Z}_v with periodic distance d . Then*

$$d \leq \left\lfloor \frac{v^2}{4(v-1)} \right\rfloor.$$

Proof. Suppose D has difference levels $\mu_1 < \dots < \mu_s = \Lambda$, and let t_i denote the number of members of the multiset $S = \{g - g' \mid g, g' \in D \text{ and } g \neq g'\}$ with multiplicity μ_i . Then we have $d = k - \Lambda$ and, counting $|S|$ in two ways, we have

$$(\Lambda - \delta_{s-1})t_{s-1} + (\Lambda - \delta_{s-2})t_{s-2} + \dots + (\Lambda - \delta_1)t_1 + \Lambda(v - 1 - t_1 - \dots - t_{s-1}) = k(k - 1)$$

where $\delta_i = \Lambda - \mu_i$. Notice we must have $1 \leq t_i \leq v$ for all i , $1 \leq i \leq s$, and all δ_i s must be nonnegative and distinct. Set $a = v - k$. Then we have

$$\Lambda = \frac{k(k - 1) + \delta_1 t_1 + \dots + \delta_{s-1} t_{s-1}}{v - 1}$$

whence

$$\begin{aligned} k - \Lambda &= v - a - \frac{(v-a)(v-a-1)}{v-1} - \frac{\delta_1 t_1 + \cdots + \delta_{s-1} t_{s-1}}{v-1} \\ &= (v-a) \frac{a}{v-1} - \frac{\delta_1 t_1 + \cdots + \delta_{s-1} t_{s-1}}{v-1}. \end{aligned}$$

By differentiating the first term of the right hand side with respect to a we find that it attains its maximum value when $a = \frac{v}{2}$. Thus we get

$$k - \Lambda \leq \frac{v^2}{4(v-1)}.$$

□

Again let D be a k -subset of \mathbb{Z}_v with periodic distance d and difference levels $\mu_1 < \cdots < \mu_s = \Lambda$. Let a, δ_i and t_i be defined as in the proof of Lemma 3.1. Suppose that

$$\left| k - \frac{v}{2} \right|^2 + \sum_{i=1}^{s-1} \delta_i t_i = \frac{v^2}{4} - (v-1) \left\lfloor \frac{v^2}{4(v-1)} \right\rfloor. \quad (5)$$

Then from the proof of Lemma 3.1 we have

$$\begin{aligned} k - \Lambda &= (v-a) \frac{a}{v-1} - \frac{\delta_1 t_1 + \cdots + \delta_{s-1} t_{s-1}}{v-1} \\ &= \frac{(\frac{v}{2} - |k - \frac{v}{2}|)(\frac{v}{2} + |k - \frac{v}{2}|) - \sum_{i=1}^{s-1} \delta_i t_i}{(v-1)} \\ &= \frac{\frac{v^2}{4} - |k - \frac{v}{2}|^2 - \sum_{i=1}^{s-1} \delta_i t_i}{(v-1)} \\ &= \frac{v^2}{4(v-1)} - \frac{|k - \frac{v}{2}|^2 + \sum_{i=1}^{s-1} \delta_i t_i}{(v-1)} \\ &= \left\lfloor \frac{v^2}{4(v-1)} \right\rfloor. \quad (\text{by (5)}) \end{aligned}$$

Together with Lemma 3.1 we have that equality holds. In fact, from the above inequality, we can see that the condition given in (5) is both necessary and sufficient. We now have a characterization of those subsets of cyclic groups for which equality holds in Lemma 3.1.

For the remainder of the paper we will denote the value $\left\lfloor \frac{v^2}{4(v-1)} \right\rfloor$ by B_v , and the peak-sidelobe distance of a binary matrix R by Q_R , or, if it is clear from the context, simply by Q . We will need the following lemma.

Lemma 3.2. *Let R be a $v \times v$ binary circulant matrix. Then $A_R(1, 0) = A_R(-1, 0) = A_R(0, 1) = A_R(0, -1)$.*

Proof. That $A_R(1,0) = A_R(-1,0)$ and $A_R(0,1) = A_R(0,-1)$ is clear. We show that $A_R(-1,0) = A_R(0,1)$. Note that for any $v \times v$ binary circulant matrix we must have $R_{i,j} = R_{v+1-j,v+1-i}$ for $1 \leq i, j \leq v$. Thus, we have

$$\begin{aligned}
A_R(0,1) &= \sum_{i=1}^v \sum_{j=1}^{v-1} R_{i,j} R_{i,j+1} + \sum_{i=1}^v R_{i,v} R_{i,v-1} \\
&= \sum_{i=1}^v \sum_{j=2}^v R_{j,i} R_{j-1,i} + \sum_{i=1}^v R_{1,i} R_{0,i} \\
&= \sum_{j=1}^v \sum_{i=1}^v R_{j,i} R_{j-1,i} \\
&= A_R(-1,0).
\end{aligned}$$

□

We are now ready to give an upper bound on the peak-sidelobe distance of a special matrix.

Theorem 3.3. *Let R be a $v \times v$ special matrix with peak-sidelobe distance Q . Then*

$$Q \leq (v+1)B_v + 1.$$

Proof. Let R have defining set D and largest difference level Λ . For any $i', \delta \in \mathbb{Z}$ we have

$$\begin{aligned}
\sum_{j=1}^v R_{i',j} R_{i',j+\delta} &\leq \begin{cases} \Lambda - 1, & \text{if } R_{i',1} = R_{i',v} = 1, \\ \Lambda, & \text{otherwise,} \end{cases} \\
&= \sum_{j=1}^v R_{i',j} R_{i',j+1}.
\end{aligned}$$

Using Lemma 3.2 it is easy to deduce that $A_R(\tau_1, \tau_2) \leq A_R(\pm 1, 0) = A_R(0, \pm 1)$ for all τ_1, τ_2 not both zero. The number of values of i' for which $R_{i',1} = R_{i',v} = 1$ is equal to the number of pairs of consecutive residues in D which, since D is special, is Λ . Thus

$$A_R(0,1) = \sum_{i=1}^v \sum_{j=1}^v R_{i,j} R_{i,j+1} = \Lambda(\Lambda - 1) + (v - \Lambda)\Lambda = (v - 1)\Lambda,$$

and

$$Q = A_R(0,0) - A_R(0,1) = vk - (v - 1)\Lambda = v(k - \Lambda) + \Lambda.$$

Note that we have $2 \leq k < v$ and $0 \leq \Lambda \leq k$. We claim that Q reaches its maximum value when $k - \Lambda$ reaches its maximum value. To see this, suppose that $k - \Lambda$ is at its maximum value and that there are k^*, Λ^* , also satisfying $2 \leq k^* < v$ and $0 \leq \Lambda^* \leq k$, such that $k^* - \Lambda^* < k - \Lambda$ and $v(k - \Lambda) + \Lambda < v(k^* - \Lambda^*) + \Lambda^*$. Then we have $v((k - \Lambda) - (k^* - \Lambda^*)) < \Lambda^* - \Lambda$ whence $v < \Lambda^* - \Lambda$,

which is impossible. This proves the claim. By Lemma 3.1, the maximum possible value of $k - \Lambda$ is B_v . From Equation (5) it is easy to deduce that $\Lambda \leq B_v + 1$ whenever $k - \Lambda = B_v$. Thus $Q \leq (v + 1)B_v + 1$, and we are done. \square

We will say that a $v \times v$ special matrix R whose peak-sidelobe distance meets the bound given in Theorem 3.3 is *s-optimal*, and we say it is *near s-optimal* if it has a peak-sidelobe distance of $(v + 1)B_v$.

4 Constructions of s-Optimal Binary Matrices from Difference and Almost Difference Sets

In this section we will use cyclotomic classes and the group ring notation introduced in Section 2. When convenient, we will denote the subset $\{b_1, \dots, b_k\} \times S$ of an additive Abelian group $A \times B$ by $\{b_1 \cdots, b_k\}S(x)$ where $S(x)$ is the polynomial in $\mathbb{Z}[A]$ corresponding to the subset S . We will only discuss those constructions which produce $v \times v$ binary circulant matrices whose peak-sidelobe distance is either $(v + 1)B_v + 1$ or $(v + 1)B_v$, i.e. either s-optimal or near s-optimal. If we take the defining set D of a binary circulant matrix R to be a (v, k, λ) difference set then, since D only has one difference level, we have that the number of pairs of consecutive residues in D is $\Lambda = \lambda$ and R is special.

Difference sets with parameters $(v, \frac{v-1}{2}, \frac{v-1}{4})$ or $(v, \frac{v+1}{2}, \frac{v+1}{4})$ are called *Paley-hadamard difference sets*. Cyclic Paley-Hadamard difference sets, up to complementation (see Theorem 2.1), include the following [1]:

- (A) with parameters $(p, \frac{p+1}{2}, \frac{p+1}{4})$, where $p \equiv 3 \pmod{4}$ is prime, and the difference set is given by $D = D_0^{(2,p)} \cup \{0\}$,
- (B) with parameters $(2^t - 1, 2^{t-1}, 2^{t-2} + 1)$, for descriptions see [5],[6],[8], [14] and [18],
- (C) with parameters $(v, \frac{v+1}{2}, \frac{v+1}{4})$, where $v = p(p + 2)$ and both p and $p + 2$ are primes. These are twin prime difference sets, and are defined by $\{(g, h) \in \mathbb{Z}_p \times \mathbb{Z}_{p+2} \mid g \neq 0 \neq h \text{ and } \chi(g)\chi(h) = -1\} \cup \{(0, h) \mid h \in \mathbb{Z}_{p+2}^*\}$ where $\chi(x) = 1$ if x is a nonzero square and $\chi(x) = -1$ otherwise [11],
- (D) with parameters $(p, \frac{p+1}{2}, \frac{p+1}{4})$, where p is a prime of the form $p = 4s^2 + 27$. These are cyclotomic difference sets and are described in [17] as $D = D_0^{(6,p)} \cup D_1^{(6,p)} \cup D_3^{(6,p)} \cup \{0\}$.

We have the following construction.

Theorem 4.1. *Let R be a $v \times v$ binary circulant matrix whose defining set is a Paley-Hadamard difference set of type (A), (B), (C) or (D). Then R is near s-optimal.*

Proof. It is a simple matter of using properties of the floor function to check that, in each of the cases (A), (B), (C) and (D), we have $k - \lambda = B_v$ and $\lambda = B_v$. \square

If we take the defining set D of a binary circulant matrix R to be a (v, k, λ, t) almost difference set, then R is special only if the number of pairs of consecutive residues in D is $\Lambda = \lambda + 1$. In many cases

it is difficult to know whether an almost difference set is special. In some cases, however, we can count the number of pairs of consecutive residues.

We will need the following lemma that can be found in [4].

Lemma 4.2. *If $q \equiv 1 \pmod{4}$ is a prime power then the cyclotomic numbers of order two are given by*

$$\begin{aligned}(0,0) &= \frac{q-5}{4}, \\ (0,1) &= (1,0) = (1,1) = \frac{q-1}{4}.\end{aligned}$$

If $q \equiv 3 \pmod{4}$ then are given by

$$\begin{aligned}(0,1) &= \frac{q+1}{4}, \\ (0,0) &= (1,0) = (1,1) = \frac{q-3}{4}.\end{aligned}$$

Theorem 4.3. *Let $p \equiv 1 \pmod{4}$ be a prime and R a $p \times p$ binary circulant matrix with defining set $D \subseteq \mathbb{Z}_p$. Then*

1. *if $D = D_0^{(2,p)} \cup \{0\}$ then R is s -optimal, and*
2. *if $D = D_1^{(2,p)}$ then R is near s -optimal.*

Proof. We show only the first case as the second case can be shown in a similar way. To see that D is special, note that, using Lemmas 2.4 and 4.2 we have

$$D(X)D(X^{-1}) = \frac{p+1}{2} \cdot \mathbf{1} + \frac{p+3}{4}D_0^{(2,p)}(X) + \frac{p-1}{4}D_1^{(2,p)}(X).$$

Since $1 \in D_0^{(2,p)}$ we have that the number of pairs of consecutive residues in D is $\Lambda = \frac{p+3}{4}$, whence D is special. It is easy to show that $k - \Lambda = B_p$ and $\Lambda = B_p + 1$ hold. \square

Note that from the proof of Theorem 5.1 one could also deduce that the defining set is an almost difference set. The next construction also uses quadratic residues. We will need the following lemma.

Lemma 4.4. [19] *Let $p \equiv 3 \pmod{4}$ be a prime. Then*

$$D = (\{0\} \times D_0^{(2,p)}) \cup (\{1, 2, 3\} \times D_1^{(2,p)}) \cup \{(0,0), (1,0), (3,0)\}$$

is a $(4p, 2p+1, p, p-1)$ almost difference set in \mathbb{Z}_{4p} .

Theorem 4.5. *Let $p \equiv 3 \pmod{4}$ be a prime. Let R be the $4p \times 4p$ binary circulant matrix with defining set*

$$D = (\{0\} \times D_0^{(2,p)}) \cup (\{1, 2, 3\} \times D_1^{(2,p)}) \cup \{(0,0), (1,0), (3,0)\} \subseteq \mathbb{Z}_{4p}.$$

Then R is s -optimal.

Proof. Let D_i denote $D_i^{(2,p)}$. To see that D is special, using Lemmas 2.4 and 4.2 we have

$$\begin{aligned}
D(X)D(X^{-1}) &= [\{0\}(D_0(X) + \mathbf{1}) + \{1, 2, 3\}(D_1(X) + \mathbf{1})] [\{0\}(D_0(X^{-1}) + \mathbf{1}) + \{1, 2, 3\}(D_1(X^{-1}) + \mathbf{1})] \\
&= \{0\}(D_0(X)D_0(X^{-1}) + D_0(X) + D_1(X) + \mathbf{1}) \\
&\quad + \{1, 2, 3\}(D_0(X)D_1(X^{-1}) + 2D_1(X)D_1(X^{-1}) + 3D_0(X) + 3D_1(X) + \mathbf{1}) \\
&= \{0\}[(1, 0) + (1, 1) + 1]D_0(X) + ((1, 1) + (1, 0) + 1)D_1(X) \\
&\quad + \{1, 2, 3\}[(0, 0) + (0, 1) + 2(1, 1) + 3]D_0(X) + ((0, 1) + (0, 0) + 2(1, 0) + 3)D_1(X) \\
&\quad + (2p + 1)\mathbf{1}.
\end{aligned}$$

If $\phi : \mathbb{Z}_{4p} \rightarrow \mathbb{Z}_4 \times \mathbb{Z}_p$ is the map given by the Chinese Remainder Theorem, it is easy to see that $\phi^{-1}((1, 1)) = 1$. Then since $1 \in D_0$, we need only consider the coefficient of $\{1\}D_0$, which is $(0, 0) + (0, 1) + 2(1, 1) + 3 = p + 1$. Thus, by Lemma 4.4, the number of pairs of consecutive residues in D is Λ , whence D is special. It is easy to show that $k - \Lambda = B_p$ and $\Lambda = B_p + 1$ hold. \square

We next show a construction from cyclotomic classes of order four. We will use the following lemmas.

Lemma 4.6. [7] *Let $q = 4f + 1$ be a prime power with f odd. The five distinct cyclotomic numbers are*

$$\begin{aligned}
(0, 0) &= (2, 2) = (2, 0) = \frac{q - 7 + 2x}{16} \\
(0, 1) &= (1, 3) = (3, 2) = \frac{q + 1 + 2x - 8y}{16} \\
(1, 2) &= (0, 3) = (3, 1) = \frac{q + 1 + 2x + 8y}{16} \\
(0, 2) &= \frac{q + 1 - 6x}{16} \\
\text{all others} &= \frac{q - 3 - 2x}{16}
\end{aligned}$$

where $q = x^2 + 4y^2$ for $x, y \in \mathbb{Z}$ with $x \equiv 1 \pmod{4}$. Here, y is two-valued depending on the choice of the primitive root α defining the cyclotomic classes (see page 400 of [4]).

Lemma 4.7. [7] *Let $p = 4f + 1 = x^2 + 4y^2$ be a prime with f odd, $x \equiv 1 \pmod{4}$ and $y = \pm 1$. Then $D_i^{(4,p)} \cup D_{i+1}^{(4,p)}$ is a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{2})$ almost difference set in \mathbb{Z}_p .*

Theorem 4.8. *Let $p = 4f + 1 = x^2 + 4y^2$ be a prime with f odd, $x \equiv 1 \pmod{4}$, and primitive element chosen so that $y = -1$. Let R be a $p \times p$ binary circulant matrix with defining set $D \subseteq \mathbb{Z}_p$. Then*

1. *if $D = D_i^{(4,p)} \cup D_{i+1}^{(4,p)} \cup \{0\}$ then R is s -optimal, and*
2. *if $D = D_i^{(4,p)} \cup D_{i+1}^{(4,p)}$ then R is near s -optimal.*

Proof. We show only the first case as the second case can be shown in a similar way. Let D_i denote $D_i^{(4,p)}$. To see that D is special, using Lemma 2.4 we have

$$\begin{aligned} D(X)D(X^{-1}) &= (D_i \cup D_{i+1} + \mathbf{1})(X)(D_i \cup D_{i+1} + \mathbf{1})(X^{-1}) \\ &= (D_i \cup D_{i+1} + \mathbf{1})(X)(D_{i+2} \cup D_{i+3} + \mathbf{1})(X) \\ &= \frac{p+1}{2} \cdot \mathbf{1} + \sum_{k=0}^3 [(2, k-i) + (3, k-i) + (1, k-i-1) + (2, k-i-1) + 1] D_k(X). \end{aligned}$$

Using properties of the cyclotomic numbers together with Lemma 4.6, we have that the coefficient of $D_0(X)$ is

$$\begin{cases} \frac{4p+4-8y}{16}, & \text{if } i = 0 \text{ or } 2, \\ \frac{4p+4+8y}{16}, & \text{if } i = 1 \text{ or } 3. \end{cases}$$

By Lemma 4.7 and Theorem 5.1 we know that $\Lambda = \frac{p+3}{4}$. Since $1 \in D_0$ we have that the number of pairs of consecutive residues in D is Λ , whence D is special. It is easy to show that $k - \Lambda = B_p$ and $\Lambda = B_p + 1$ hold. \square

5 Contruction of Binary Matrices with Good Peak-Sidelobe Distances

In this section we give a construction of binary matrices with good peak-sidelobe distances from s-optimal matrices by following the strategy mentioned in Section 1.2. Let R be a $(v-2) \times (v-2)$ s-optimal matrix with defining set D of cardinality k . Then, by Theorem 3.3, R has peak-sidelobe distance $(v-1)B_{v-2} + 1$. Let R' be the $v \times v$ matrix obtained by adjoining a border of 1s to R . i.e.

$$R' = \begin{bmatrix} 1 & \cdots & 1 \\ \vdots & R & \vdots \\ 1 & \cdots & 1 \end{bmatrix}.$$

Since the nearest sidelobe of R occurs in $\{A_R(\pm 1, 0), A_R(0, \pm 1)\}$, and R is circulant, it is easy to see that the nearest sidelobe of R' must occur in $\{A_{R'}(\pm 1, 0), A_{R'}(0, \pm 1)\}$ and that the peak-sidelobe distance of R' is given by

$$Q_{R'} = A_{R'}(0, 0) - A_{R'}(\pm 1, 0) = A_{R'}(0, 0) - A_{R'}(0, \pm 1) = (v-1)B_{v-2} + 2(v-k) + 1.$$

Now fix $a, b \in \{1 \dots v\}$ and define $S_{aj}^b = \{(a, j) \mid 2 \leq j \leq v-1, R'_{bj} = 1\}$ and $S_{ia}^b = \{(j, a) \mid 2 \leq i \leq v-1, R'_{ib} = 1\}$. Then the exterior entries of the matrix R' having adjacent interior entries equal to 1 can be represented by the sets $S_{1j}^2, S_{vj}^{v-1}, S_{i1}^2$ and S_{iv}^{v-1} . Now modify R' by choosing one entry from each of $S_{1j}^2, S_{vj}^{v-1}, S_{i1}^2$ and S_{iv}^{v-1} , and changing it to 0. Let I denote the set of indices for the four chosen entries, and R'_I denote the resulting matrix. It is straightforward to show that the nearest sidelobe of R'_I occurs in $\{A_{R'_I}(\pm 1, 0), A_{R'_I}(0, \pm 1)\}$ and that R'_I has peak-sidelobe distance given by $Q_{R'_I} = (v-1)B_{v-2} + 2(v-k) + 3$. Similarly, if R is near s-optimal then R'_I has peak-sidelobe distance $Q_{R'_I} = (v-1)B_{v-2} + 2(v-k) + 2$. We thus have the following.

Theorem 5.1. Let R be a $(v-2) \times (v-2)$ special matrix with defining set D of cardinality k , and let I contain exactly one index from each of $S_{1j}^2, S_{vj}^{v-1}, S_{i1}^2$ and S_{iv}^{v-1} . Then R'_I is a $v \times v$ binary matrix with peak-sidelobe distance

$$Q_{R'_I} = \begin{cases} (v-1)B_{v-2} + 2(v-k) + 3, & \text{if } R \text{ is } s\text{-optimal,} \\ (v-1)B_{v-2} + 2(v-k) + 2, & \text{if } R \text{ is near } s\text{-optimal.} \end{cases}$$

Example 5.2. Let D be the set of quadratic nonresidues in \mathbb{Z}_5 and R the binary circulant matrix with defining set D . Then $S_{1j}^2 = \{(1,4), (1,5)\}$, $S_{vj}^{v-1} = \{(7,3), (7,4)\}$, $S_{i1}^2 = \{(4,1), (5,1)\}$ and $S_{iv}^{v-1} = \{(3,7), (4,7)\}$. Take $I = \{(1,4), (7,4), (4,1), (4,7)\}$. Then we have

$$R = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad R'_I = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

By Theorem 4.1, R is near s -optimal, and so by Theorem 5.1 we have that the peak-sidelobe distance of R'_I is $Q_{R'_I} = (v-1)B_{v-2} + 2(v-k) + 2 = 18$. According to [15], an optimal 7×7 binary matrix has peak-sidelobe distance 19.

Example 5.3. Let D be the set of quadratic residues in \mathbb{Z}_7 and R the binary circulant matrix with defining set $D \cup \{0\}$. Then $S_{1j}^2 = \{(1,2), (1,3), (1,4), (1,6)\}$, $S_{vj}^{v-1} = \{(9,2), (9,5), (9,4), (9,6)\}$, $S_{i1}^2 = \{(2,1), (5,1), (7,1), (8,1)\}$ and $S_{iv}^{v-1} = \{(2,9), (5,9), (7,9), (8,9)\}$. Take $I = \{(1,4), (9,5), (5,1), (6,9)\}$. Then we have

$$R = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad R'_I = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

By Theorem 4.1, R is near s -optimal, and so by Theorem 5.1 we have that the peak-sidelobe distance of R'_I is $Q_{R'_I} = (v-1)B_{v-2} + 2(v-k) + 2 = 28$. According to [15], the best peak-sidelobe distance for a 9×9 binary matrix is 29.

Remark 5.1. Note that in the two examples given above, although we have chosen the set I so that the resulting matrix R'_I is symmetric, a different choice of the set I will have no effect on the peak-sidelobe distance as long as the condition in the statement of Theorem 4.1 is satisfied.

Remark 5.2. Also note that a square binary matrix constructed via Theorem 5.1 from an s -optimal interior matrix does not necessarily have a greater peak-sidelobe distance than one constructed from a near s -optimal interior matrix. This can easily be seen by comparing the matrices that result from applying Theorem 5.1 to interior matrices constructed using parts (1) and (2) of either of Theorems 4.3 and 4.8.

We have computed the best peak-sidelobe distances of square binary matrices constructed via Theorem 5.1 of orders between 7 and 19 and included them in Table 1. We have also computed explicitly the parameters and peak-sidelobe distances for the infinite families of square binary matrices constructed in this paper and included them in Table 2.

6 Concluding Remarks

We have shown how difference sets and almost difference sets can be used to construct binary matrices with peak-sidelobe distances that are good in the sense that, for small dimension (as illustrated in Examples 5.2 and 5.3), are very close to being optimal. Before this paper, there have been no results on deterministically constructing such families of binary matrices and, so far, have only been constructed via exhaustive computer searches. We have formulated a tight general upper bound on the peak-sidelobe distance of a certain class of circulant matrices whose defining sets are difference sets and almost difference sets. By using circulant matrices whose aperiodic autocorrelations meet this upper bound, we were able to construct square binary matrices with good aperiodic autocorrelation properties. We leave the reader with the following open problems: 1) Formulate a tight general upper bound on the peak-sidelobe distance of a square binary matrix or, improve on the upper bound formulated by Skirlo et al. in [15], 2) Find new ways of constructing square binary matrices with good aperiodic autocorrelation properties.

Table 1: Table of peak-sidelobe distances of square binary matrices constructed via Theorem 5.1 of orders between 7 and 19.

Note: 'DS' and 'ADS' refer to 'difference set' and 'almost difference set' respectively.

Note: Orders given with a '*' refer to those for which previous results exist and for which comparisons are made in Examples 5.2 and 5.3.

Order M	Ref. to construction of $(M-2) \times (M-2)$ interior	Param. of DS or ADS used as defining set D of R	Peak-sidelobe distance $Q_{R'_I}$ of $M \times M$ matrix R'_I
7*	Theorem 4.3 part(2)	(5, 2, 0, 2)-ADS	18
9*	Theorem 4.1	(7, 4, 2)-DS	28
13	Theorem 4.1	(11, 6, 3)-DS	52
14	Theorem 4.5	(12, 7, 3, 2)-ADS	56
15	Theorem 4.3 part(2), Theorem 4.8 part(2)	(13, 6, 2, 6)-ADS	62
17	Theorem 4.1	(15, 8, 4)-DS	84
19	Theorem 4.3 part(2), Theorem 4.8 part(2)	(17, 8, 3, 8)-ADS	96

Table 2: Table of parameters of families of square binary matrices constructed via Theorem 5.1.

Note: 'DS' and 'ADS' refer to 'difference set' and 'almost difference set' respectively.

Ref. to construction of $(M - 2) \times (M - 2)$ interior	Param. of DS or ADS used as defining set D of R	Peak-sidelobe distance $Q_{R'_I}$ of $M \times M$ matrix R'_I
Theorem 4.1	$(v, \frac{v+1}{2}, \frac{v+1}{4})$ -DS of Paley-Hadamard type $(A), (B), (C)$ or (D)	$(v + 1) \left(\left\lfloor \frac{v^2}{4(v-1)} \right\rfloor + 1 \right) + 4$
Theorem 4.3 part(1), Theorem 4.8 part(1)	$(p, \frac{p+1}{2}, \frac{p-1}{4}, \frac{p-1}{2})$ -ADS of where $p \equiv 1 \pmod{4}$ is prime	$(p + 1) \left(\left\lfloor \frac{p^2}{4(p-1)} \right\rfloor + 1 \right) + 5$
Theorem 4.3 part(2), Theorem 4.8 part(2)	$(p, \frac{p+1}{2}, \frac{p-1}{4}, \frac{p-1}{2})$ -ADS of where $p \equiv 1 \pmod{4}$ is prime	$(p + 1) \left(\left\lfloor \frac{p^2}{4(p-1)} \right\rfloor + 1 \right) + 6$
Theorem 4.5	$(4p + 1, 2p + 1, p, p - 1)$ -ADS where $p \equiv 3 \pmod{4}$ is prime	$(4p + 1) \left(\left\lfloor \frac{4p^2}{4p-1} \right\rfloor + 1 \right) + 4$

References

- [1] K.T. Arasu, C.Ding, T. Hellesteth, P.V. Kumar, and H.M. Martinsen. Almost difference sets and their sequences with optimal autocorrelation. *IEEE Trans. Inform. Theory*, 47:2934–2943, 2001.
- [2] R. H. Barker. Group synchronizing of binary digital systems. *W.J. Communication Theory, Ed.*, 1990.
- [3] V. Boegli and D. P. Kern. Automatic mark detection in electron-beam nanolithography using digital image processing and correlation. *J. Vacuum Science Technology*, 8(6):1994–2001, 1990.
- [4] L.E. Dickson. Cyclotomy, higher congruences and Waring's problem. *Amer. J. Math.*, 57:391–424, 1935.
- [5] J. F. Dillon. Multiplicative difference sets via additive characters. *Des., Codes Cryptogr.*, 17:225–235, 1999.
- [6] J. F. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields Appl.*, 10(3):342–389, 2004.
- [7] C. Ding, T. Hellesteth, and H. Martinsen. New families of binary sequences with optimal three-level autocorrelation. *IEEE Trans. Inform. Theory*, 47(1):428–433, 2001.
- [8] B. Gordon, W. H. Mills, and L.R. Welch. Some new difference sets. *Canadian J. Math.*, 14:614–625, 1962.
- [9] S. R. Gottesman and E. E. Fenimore. New family of binary arrays for coded aperture imaging. *Applied Optimization*, 28(20):4344–4352, 1989.
- [10] Marshall Hall Jr. A survey of difference sets. *Proc. AMS*, 7:975–986, 1956.

- [11] D. Jungnickel and A. Pott. Difference sets: An introduction. In A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, editors, *Difference Sets, Sequences and Their Correlation Properties*, pages 259–295. Amsterdam, The Netherlands: Kluwer, 1999.
- [12] F. Neuman and L. Hoffman. New pulse sequences with desirable correlation properties. *IEEE Aerospace and Electronic Sys.*, AES7(3):570, 1971.
- [13] K. Nowak. A survey on almost difference sets. *arXiv:1409.0114v1*, 2014.
- [14] A. Pott. *Finite Geometry and Character Theory (Lecture Notes in Mathematics)*, volume 1601. Berlin, Germany: Springer-Verlag, 1995.
- [15] S. Skirlo, Ling Lu, and M. Soljacic. Binary matrices of optimal autocorrelation as alignment marks. *arXiv:1408.6915v1*, 2014.
- [16] D.R. Stinson. *Combinatorial Designs: Constructions and Analysis*. SpringerVerlag, 2003.
- [17] T. Storer. *Cyclotomy and Difference Sets*, pages 65–72. Markham, Chicago, 1967.
- [18] Q. Xiang. Recent results on difference sets with classical parameters. In A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, editors, *Difference Sets, Sequences and Their Correlation Properties*, pages 419–434. Amsterdam, The Netherlands: Kluwer, 1999.
- [19] Y. Zhang, J.G. Lei, and S.P. Zhang. A new family of almost difference sets and some necessary conditions. *IEEE Trans. Inform. Theory*, 52(5):2052–2061, 2006.